DATAPOWER

XML-aware Network Infrastructure

Eugene Kuznetsov
Chairman & CTO
DataPower Technology, Inc.
http://www.datapower.com

Agenda

- Won't talk about applications, software, tools or platforms…
- Web services are also about networks
- Talk about network infrastructure:
  - Network equipment
  - Network services
- New protocols create new pressures and demands on existing networks

- Challenges
  - Performance
  - Security
  - Expense
- A new approach

Performance Challenge

- XML is a text-based self-tagging format
- Same messages up to 20 times larger than binary
- Example:
  - 0xA13FF51301 [5 bytes] →
  - <?xml version="1.0" ?> <invoice><no>1001</no> <product><sku>150591501</sku></product></invoice> [95 bytes]
- Variable length fields, variable encodings
- Complex processing model – XPath, XML Security, SOAP
- Result:
  - Some XML apps literally grind to a halt
  - Website pages taking 10 seconds to load
  - More and more hardware required

Current Approach to XML Performance

- Buy more general-purpose server hardware
  - $ to purchase, $$$ to operate
- Avoid XML/SOAP for high-speed systems
- Use non-standard “subset” of XML
  - defeats interoperability, costs more in the end
- Cut out application features
  - undercuts business objective for using XML
- Hand-tune the XML processing software in the app
  - takes a long time for even minor improvements
  - expensive programming resources
  - every minute spent on “XML stack” is a minute not invested in core application

Need to make XML Web Services FASTER and CHEAPER

Security Challenge

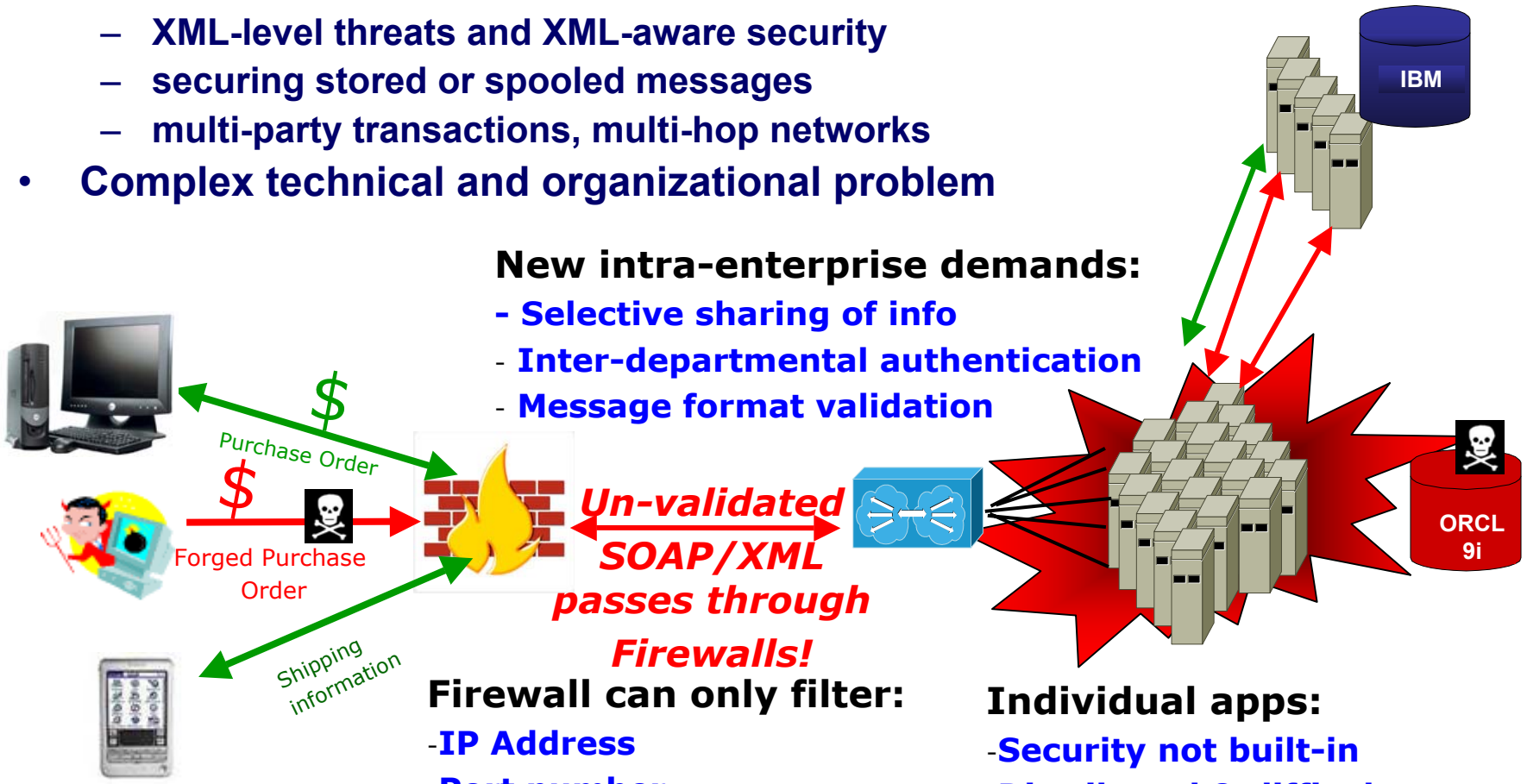
- New connectivity → new risks
- How is XML/WS different than current systems?
- The very value of XML Web Services comes from connecting sensitive systems
- Technology much more flexible and powerful than previously widely deployed
- SOAP designed to bypass existing network security infrastructure

- *"Implementation of Microsoft SOAP, a protocol running over HTTP precisely so it could bypass firewalls, should be withdrawn. According to the Microsoft documentation: "Since SOAP relies on HTTP as the transport mechanism, and most firewalls allow HTTP to pass through, you'll have no problem invoking SOAP endpoints from either side of a firewall."* – Bruce Schneier

- Why is SOAP designed to do this?

Why a new security model?

- XML and SOAP easily expose backend systems
- Selectively share data inside ***and*** outside the enterprise
- Today's security tools do not secure XML/SOAP
- SSL is not the answer
  - XML-level threats and XML-aware security
  - securing stored or spooled messages
  - multi-party transactions, multi-hop networks
- Complex technical and organizational problem



New intra-enterprise demands:

- Selective sharing of info
- Inter-departmental authentication
- Message format validation

Un-validated SOAP/XML passes through Firewalls!

Firewall can only filter:

- IP Address
- Port number
- Protocol

Individual apps:

- Security not built-in
- Distributed & difficult to secure

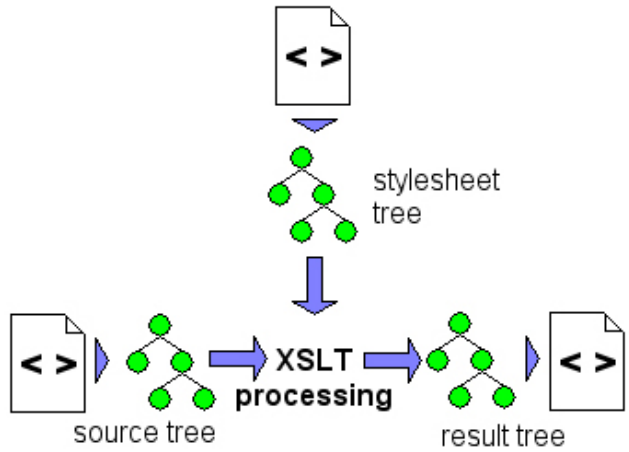
DATAPOWER

“Internal” Systems

- A lot of XML and XML web services “inside the firewall” → no security needs?
- Pilot mode web services
- Erosion of enterprise perimeter
- Insider attack risk
- Selective information sharing
- Auditability
- “Semi-trusted” environments
- Regulatory / policy requirements
- Internal → external
- Architectural choices
  - Spend time upfront on security
  - Get pilot up and audit/secure code later

Technology and Specifications

- **Foundation**
  - XML
  - SOAP
  - XPath/XSLT
  - XSD
- **Security Building Blocks**
  - XML Digital Signature
  - XML Encryption
- **Upper-Layer Protocols/Standards**
  - WS-Security
  - SOAP Security
  - XKMS
  - SAML
  - XACML
- **Not in themselves solutions**
  - Rapidly mutating



Overview of Challenges and Choices

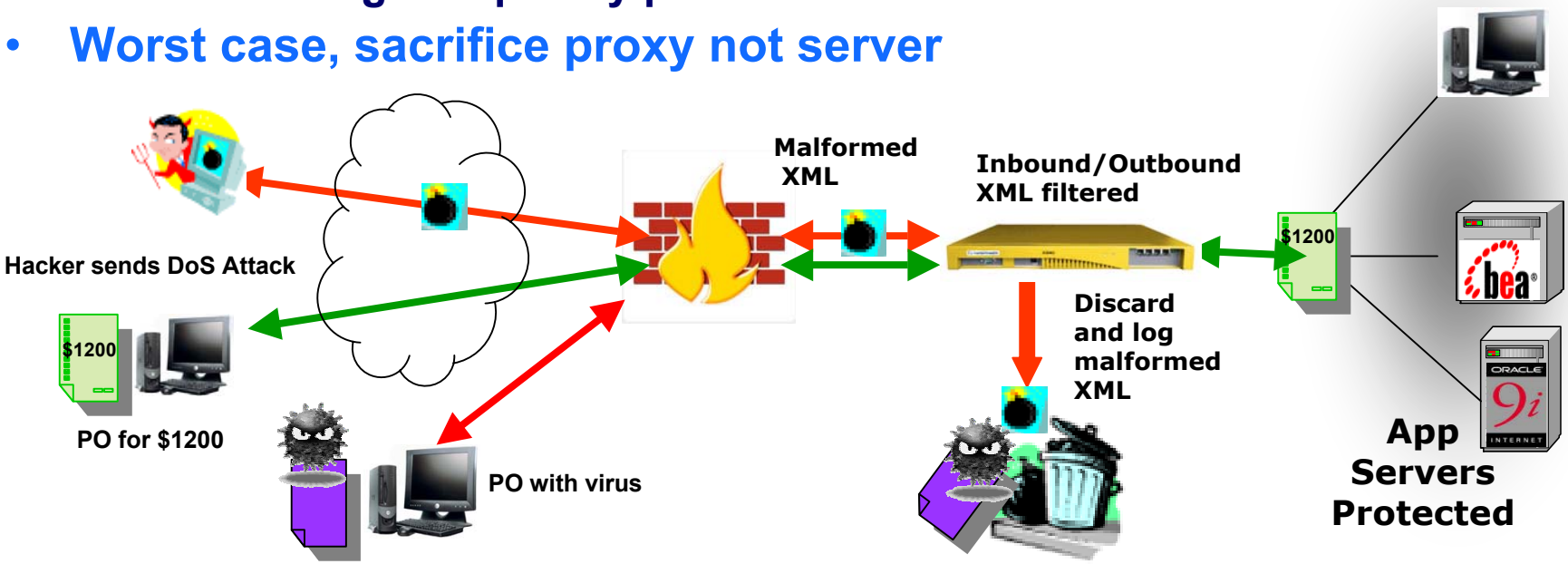
- New technology, rapidly changing standards
  - Lack of strategic clarity, lots of marketing noise
  - Many immature products and architectures
  - Getting and staying on top technology changes, training staff
  - Very broad set of potential threats
- Organizational challenges
  - Who is responsible for XML/WS security?
  - Pressure to get new apps into production
  - Trading partners, business units
- Is there anything rational to be done?
- Architectural choices
  - Spend a lot of time upfront on security?
  - Get pilot app up and audit/secure code later?
  - Code all XML security into the app?
  - Write one's own XML proxy software, install on server in DMZ?
  - Who would manage security operations in production?
- A security breach is very expensive

Need to make XML Web Services SAFER

DataPower

Network-Style Risks: XDoS

- Once theoretical, real XML DoS On the Rise
  - Malformed DTDs create infinite loop[1]
  - Affects Apache, BEA, IBM Websphere, Macromedia and others
- Unlike TCP DoS, one XML request enough for XDoS
  - Low bandwidth & undetected by firewalls
- Typical filters
  - Content match
  - Limit request/connection duration
  - Set message frequency profiles
- Worst case, sacrifice proxy not server

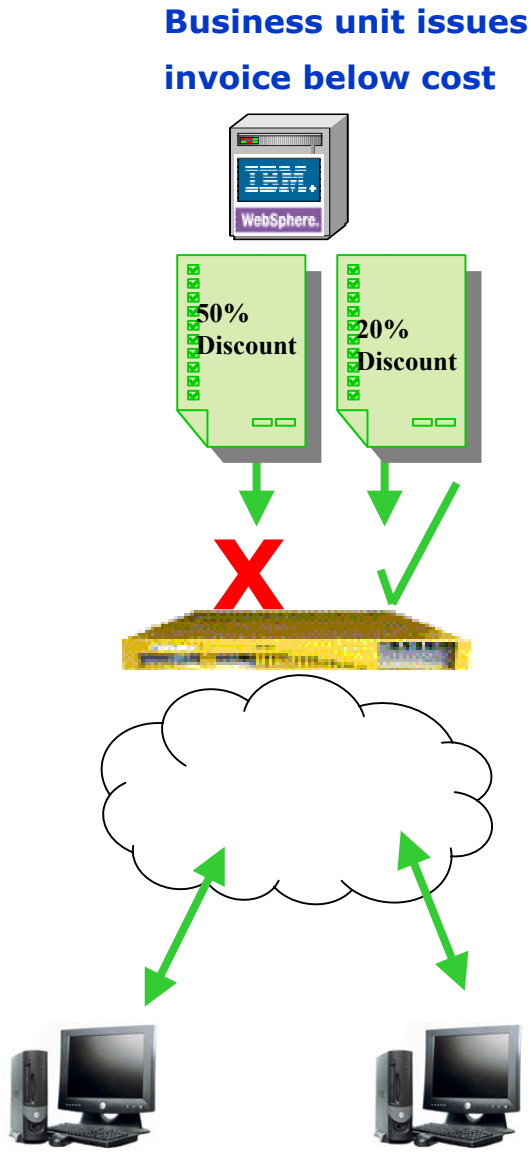


DATAPOWER

[1] SecurityTracker, Xerces XML Parser Bug in Handling DTDs May Let Users Cause Denial of Service Conditions, November 2002

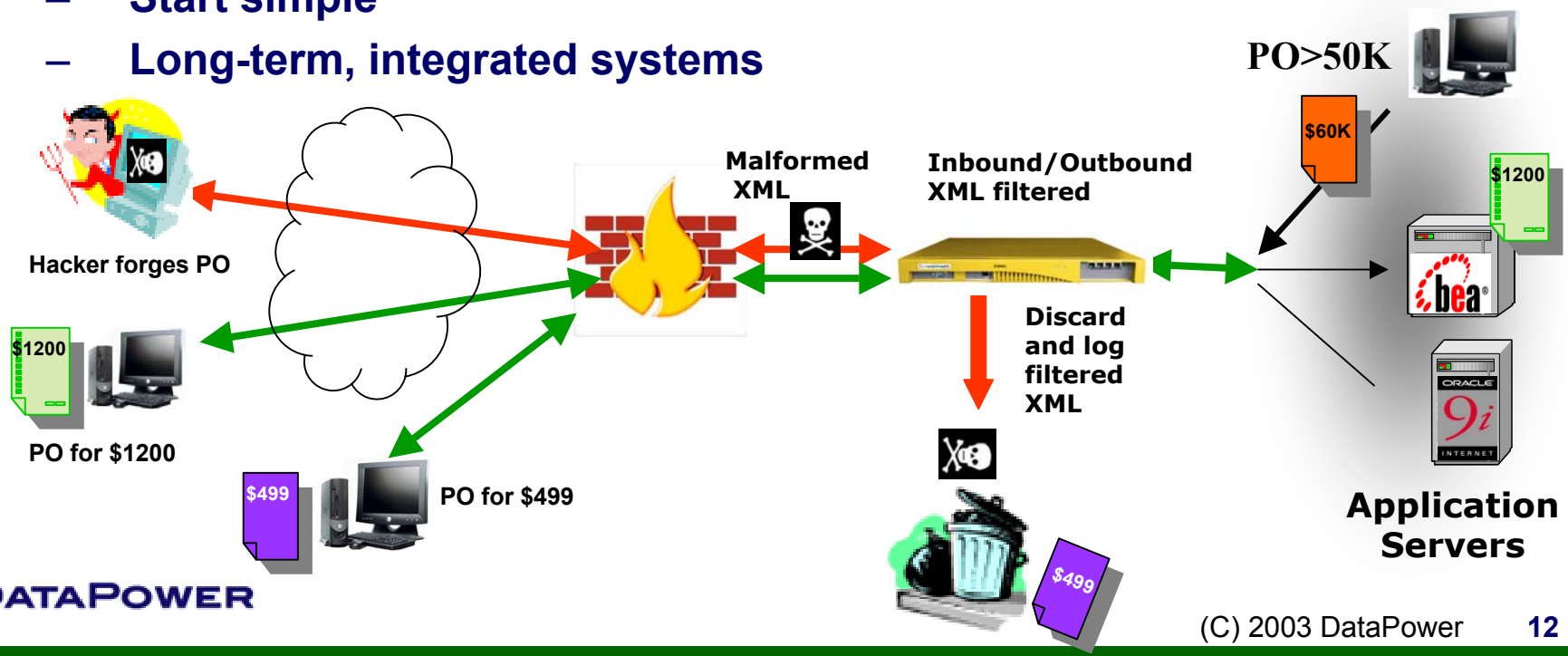
App-Style Risks: Invalid Messages

- Schema validation - ensure only known good requests enter and leave enterprise
- Prevent disruptions of server apps triggered by unexpected messages
- Messages checked for:
  - XML well-formedness
  - Improper entity or resource references
  - Protocol (e.g. SOAP) validity
  - other risks at message-validity level
- WSDL as validity template
- Beware of performance impact of validation (4X or more)



App-Style Risks: Access Violates Policy

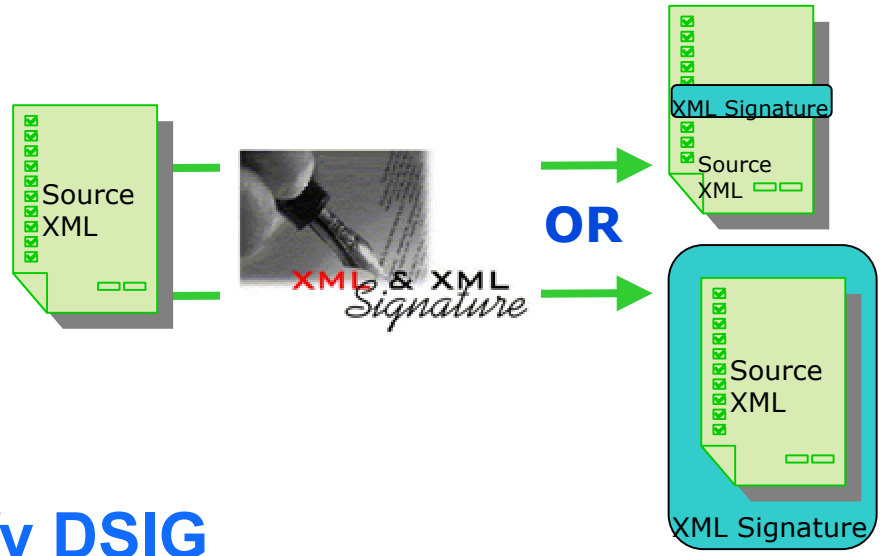
- Enforce business policies
  - No orders over $50K can leave network
  - No incoming POs for less than $500
  - Quality-of-Protection based on content
- Change filters to counter new threats
  - Can use XPath/XSLT for business-level policy
- Access control
  - Start simple
  - Long-term, integrated systems



DataPower

App-Style Risk: Message Tamper, Snooping

- **XML DSIG Provides:**
  - Tampering protection
  - Auditing & non-repudiation
- **Verify message origin**
  - Prevent spoofing
- **Recipients optionally verify DSIG**
- **Easily implemented**
  - Signature within message
  - Message within signature



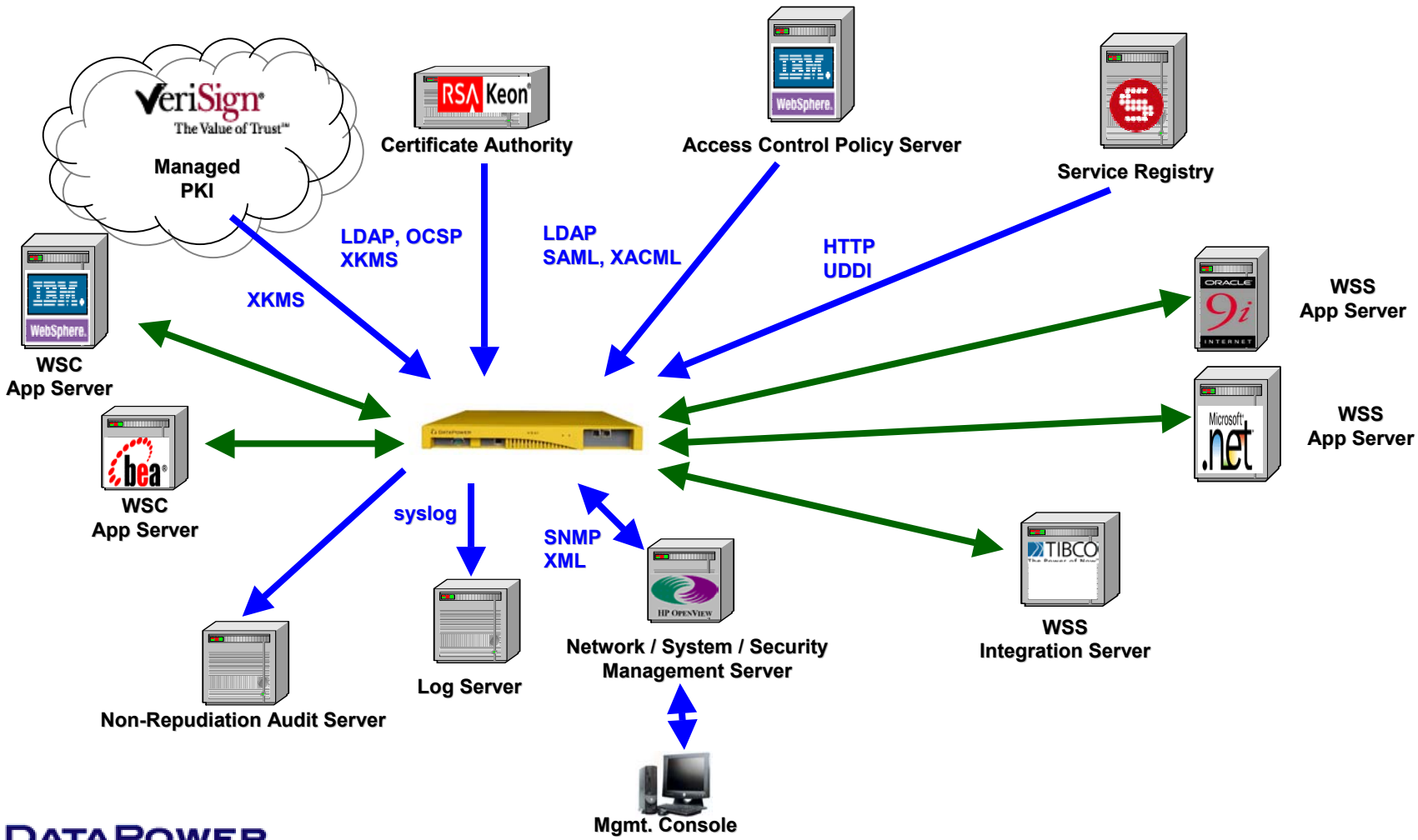
DSIG Challenges

- So many standards
- Where to place signature
  - Enveloped, enveloping, detached
- SOAP helps but not enough
  - SOAP Security, WS-Security
- So Many Crypto Choices
  - RSA/DSA/HMAC, SHA/SHA256
- So many canonicalization:
  - C14n, exc-c14n, SOAP normalization, UDDI's Schema C14n

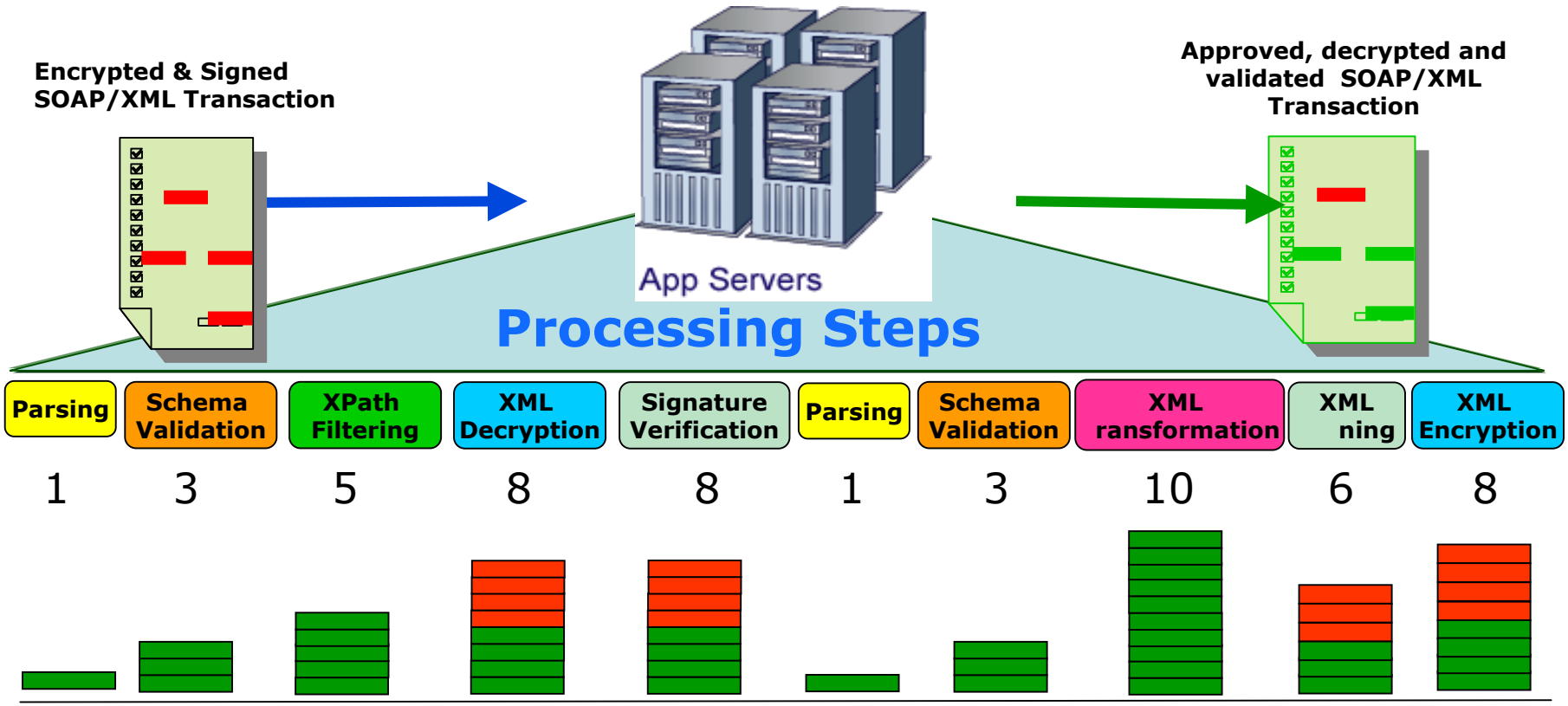
Interoperability is Hard!

XML Security Deployment Ecosystem

- External PKI infrastructure: CA servers, services
- Application Infrastructure: web servers, application servers, integration servers
- Management Infrastructure: systems, network, security and logging



Comprehensive XML Security is Resource Intensive



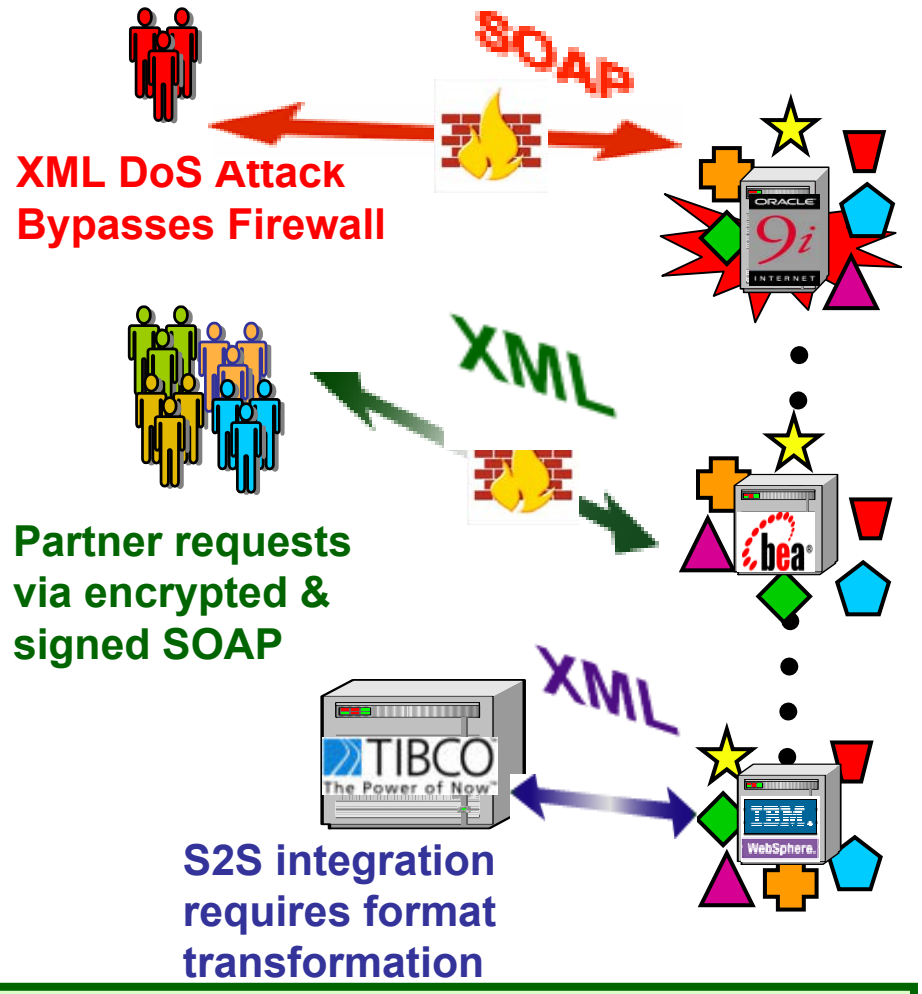
- **Performance is key to security**
  - Each security function requires XML processing
  - Must implement all practices without any compromise
  - Need ability to scale as content and user base grows

Need to make XML Web Services Security FASTER

DataPower

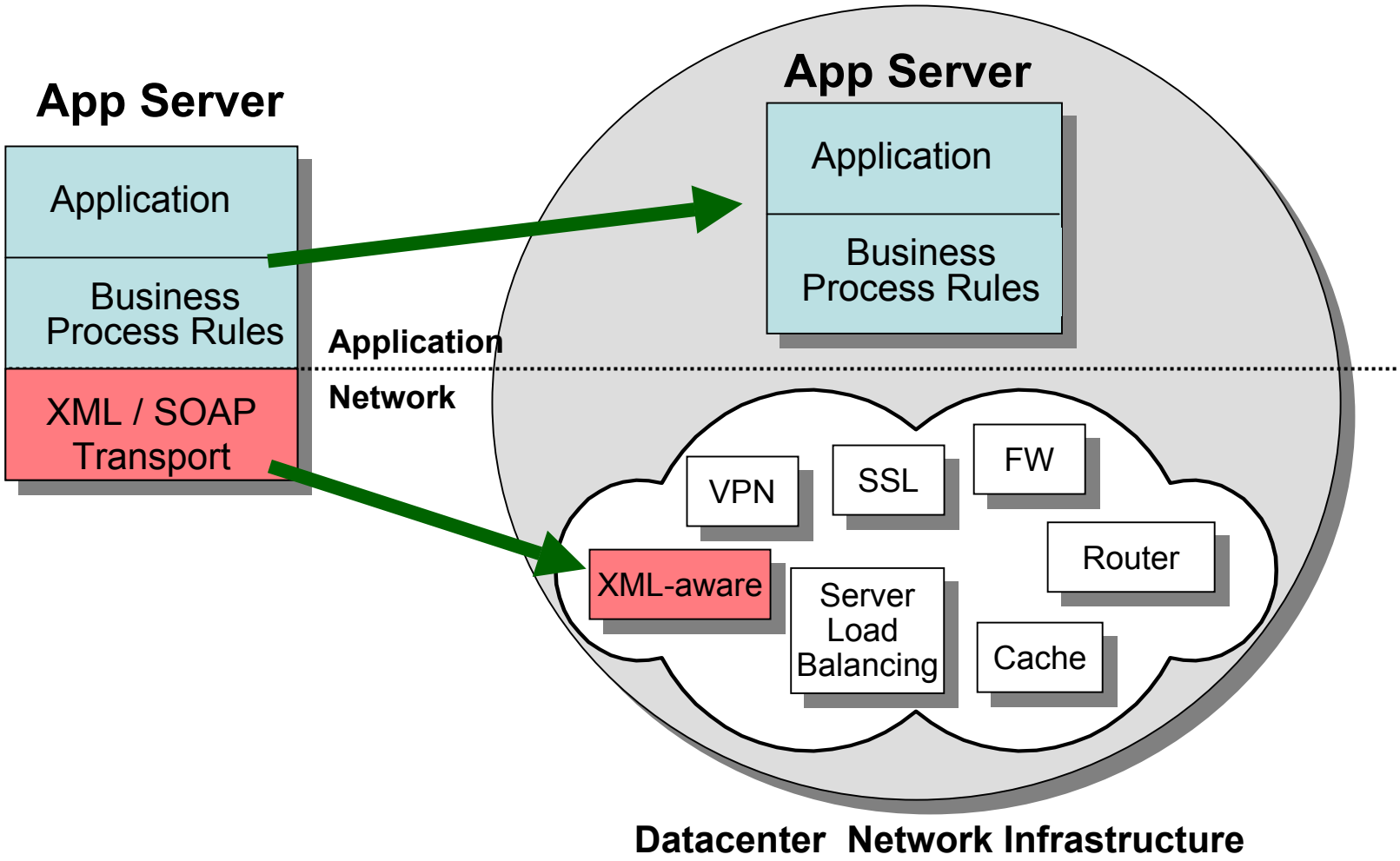
Current XML Sec. Approach -- in App. Software

- **New, Unfamiliar Tasks**
  - XML/SOAP bypasses firewalls
  - Apps must now provide security
  - Which specs? SDK?
- **Code-intensive**
  - Constant security patches
  - Endless debugging and performance tuning
- **Code audits!**
  - Prove app complies w. central security policy
  - Change app as policies change
- **Poor Performance**
  - "Commodity" functions swamp servers
  - Apps "dumbed down" or stay in pilot
- **Capital Costs**
  - Duplication of effort
  - Overprovisioned CPU & memory



Need to make XML Web Services SAFER and CHEAPER

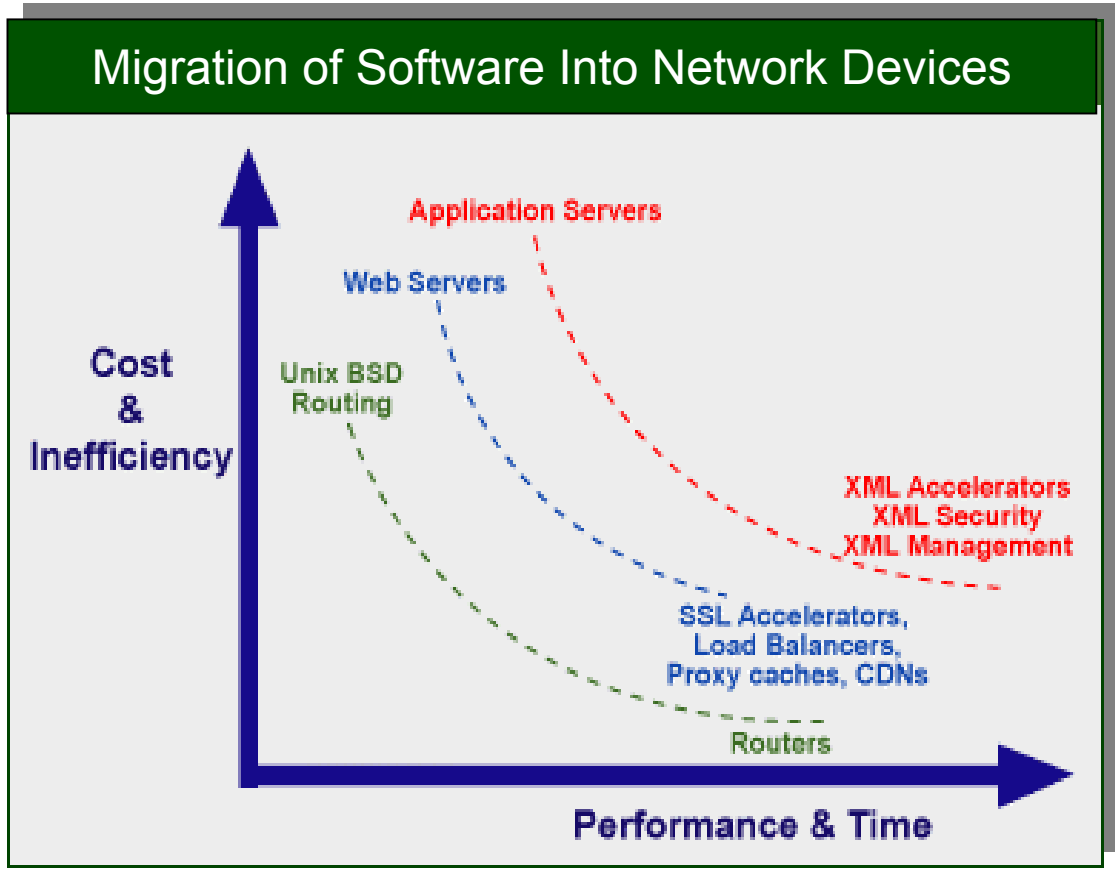
New Approach:
Offload to XML-aware network devices



DataPower

Put it all of this and more into the app?

- Code it into every app and maintain it forever
- Could write a software server, get network ops to maintain it
- Instead, take advantage of historical trend!
- Network devices getting smarter over time:
  - Gateways, routers, NAT
  - SSL Accelerators
  - Caches, CDNs
  - Server Load Balancers
- Leverage this trend
  - XML-Aware Network Devices



Benefits of the XML-aware Networking Approach

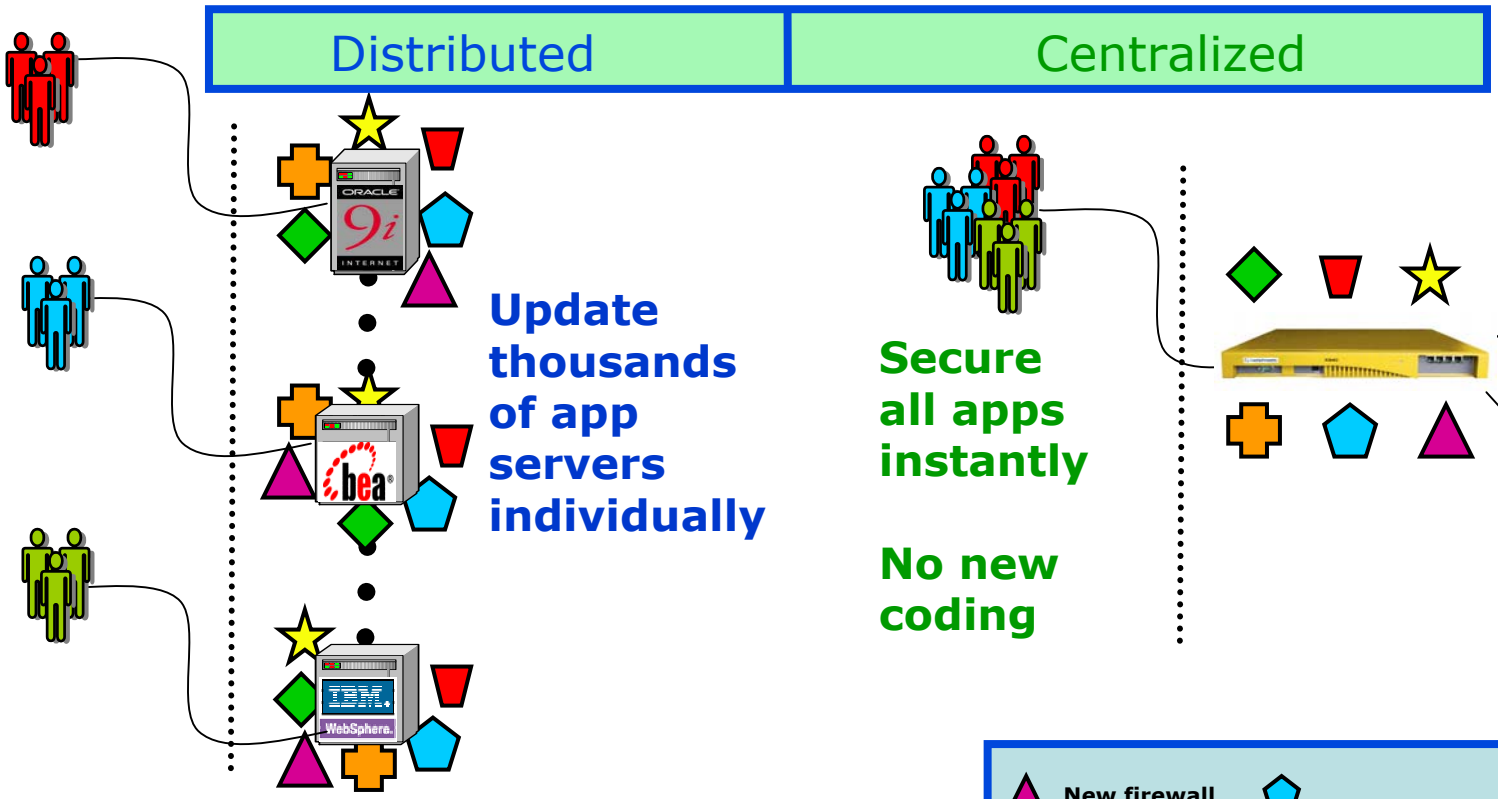
- CIOs & CSOs
  - Cut ownership costs
  - Enhanced security
  - Leverage current investments
- Application Architects
  - Enhanced security
  - Reduced debugging cycles
  - Simplified deployments
- Network Managers
  - Instant XML-aware security without programming
  - Improved uptime
  - Fewer servers and less complexity

XML hardware encourages interoperability

- Coupled to the other systems by Ethernet jack, not custom code
- Separation of concerns
- Network gear business model based on “out-of-the-box” interop
- Large software vendors focused on creating XML-enabled platforms
  - Functionality and development tools benefit
  - Interop is necessarily secondary, standards wars looming
- Network vendors architecturally unable to achieve “lock-in”
- Focused on a concrete set of challenges
  - XML security performance
  - Interoperability.

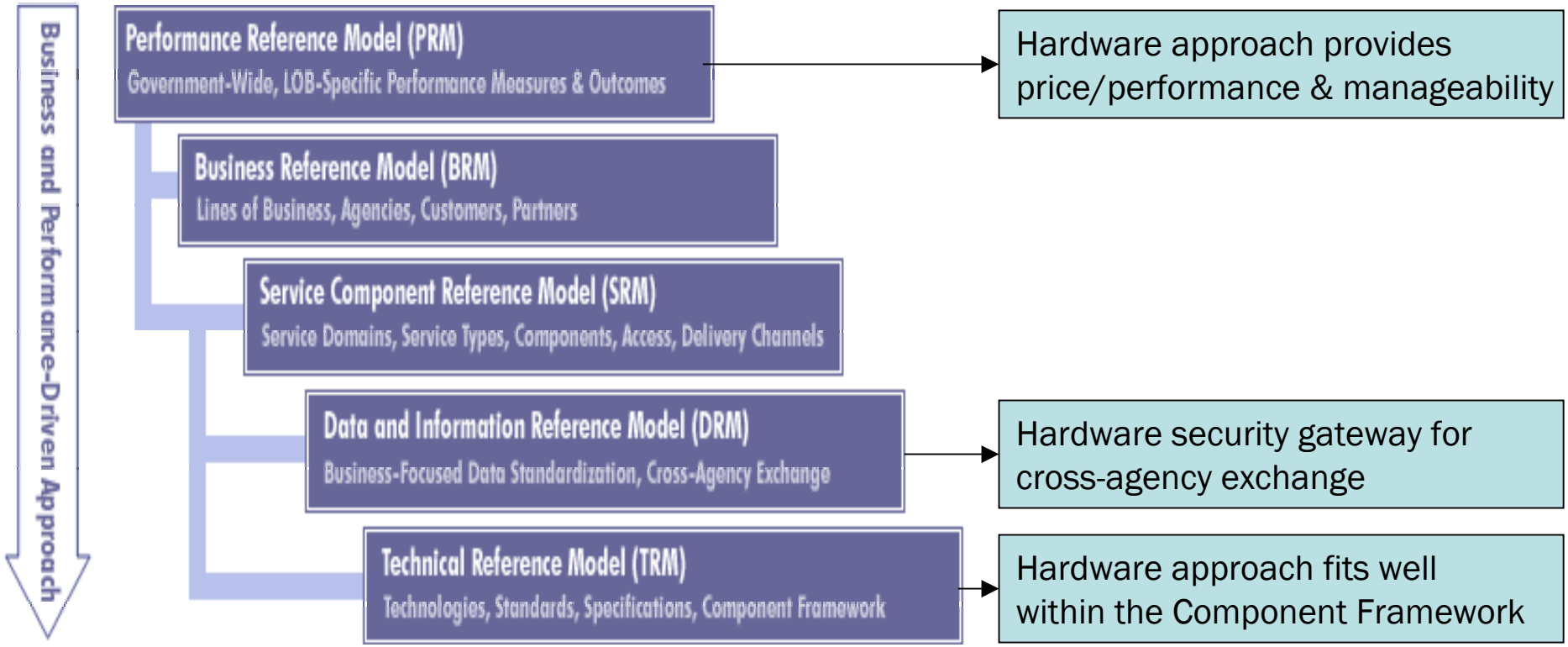
Centralized Security Deploys Easily

- XML-Aware Networking centralizes security
  - Secure multiple apps without multiple code changes
  - Boost performance while reducing cost and complexity
  - Perform security functions ***before*** they reach app servers



DATAPOWER

XML-aware Network Hardware and FEA



DataPower

DataPower's XA35 and XS40

XML Aware Network Devices

XA35 XML Accelerator

- Improve application performance by 10X or more
- Reduce development cycles with uniform infrastructure
- Slash capital and ownership costs
- Infrastructure Product of the Year

XS40 XML Security Gateway

- Includes all the capabilities of XA35
- Industry's fastest XML security
- Most comprehensive XML Web Services security functions
- Most "AGILE"; adapts to standards, apps & policies

Hardware XML Security Customer Example

COMMONWEALTH OF MASSACHUSETTS
Department of Revenue

Business Goal: MADoR has spent the past year redesigning the tools business taxpayers use to comply with the Commonwealth's tax filing and payment requirements. On July 1, 2003, DOR rolled out the first phase of the new "**WebFile for Business"** with an enhanced filing platform that gives taxpayers the expanded functionality they need.

Technology Needs XS40 Solved:

- Comprehensive Web Service security
- Superior application performance
- Bullet-proof security for Microsoft .NET-based XML Web Services
- Centralized, easy to implement solution
- Robust security, fastest processing speed and ease of use were critical.

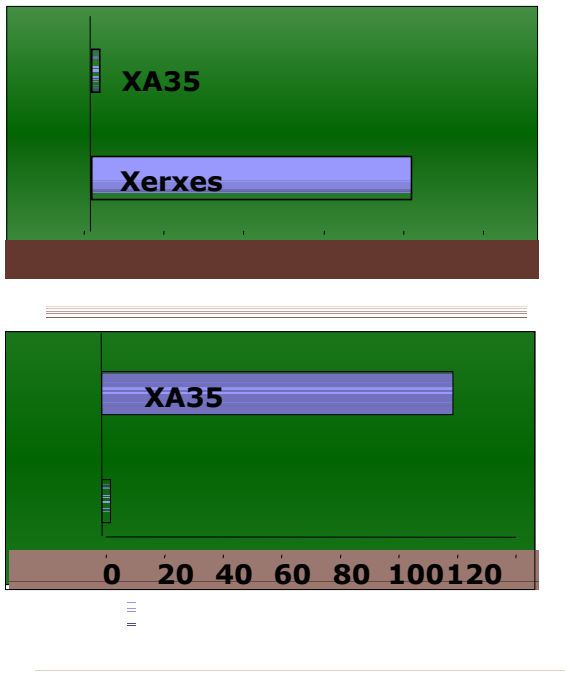
DataPower

Hardware XML Acceleration Customer Example

Hemscott – The number one provider of corporate investor relations web sites in the United Kingdom

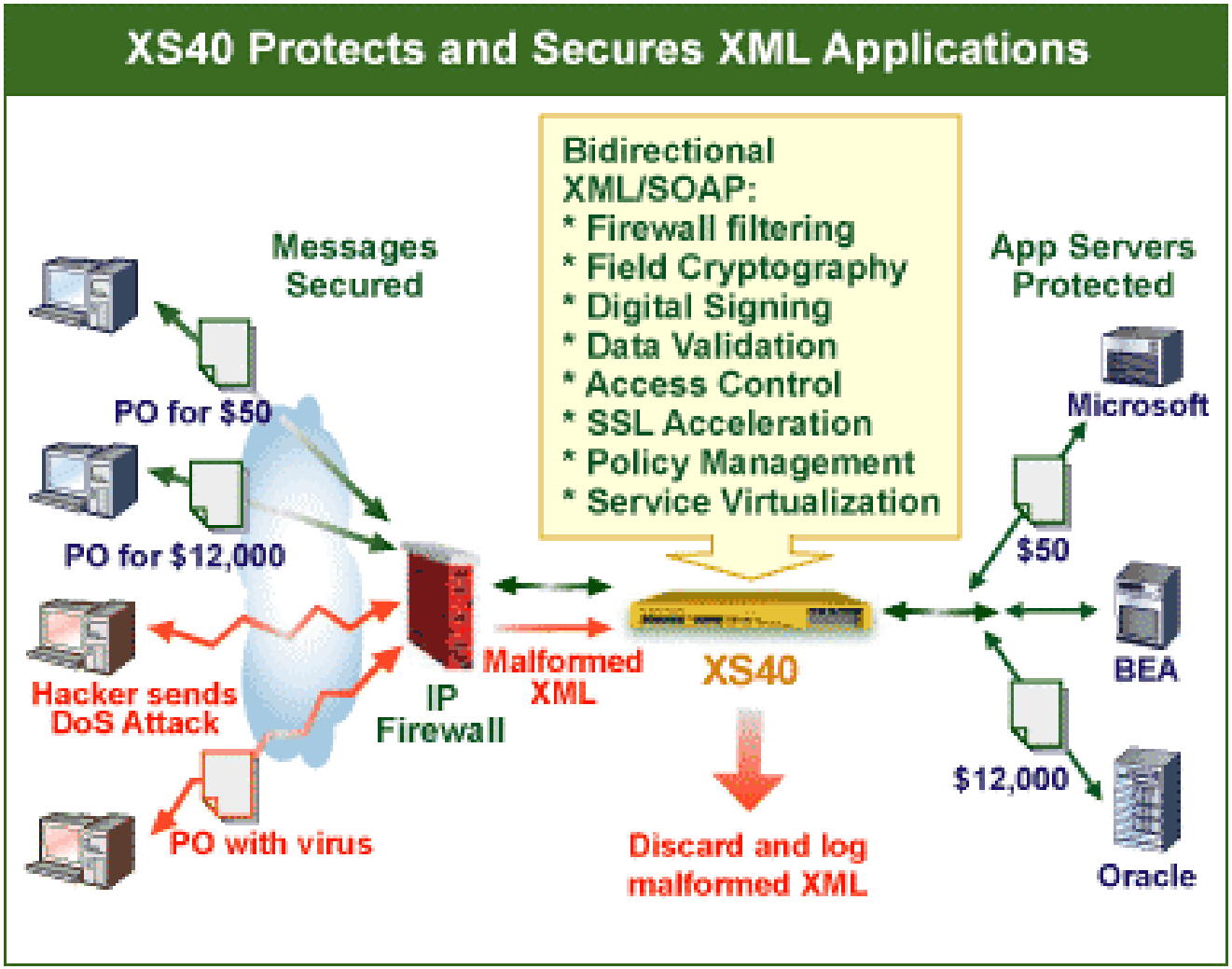
"Only DataPower XA35 is without peer when it comes to processing and accelerating XML. DataPower order-of-magnitude performance difference over software approaches keeps Hemscott clients one step ahead of their competition."

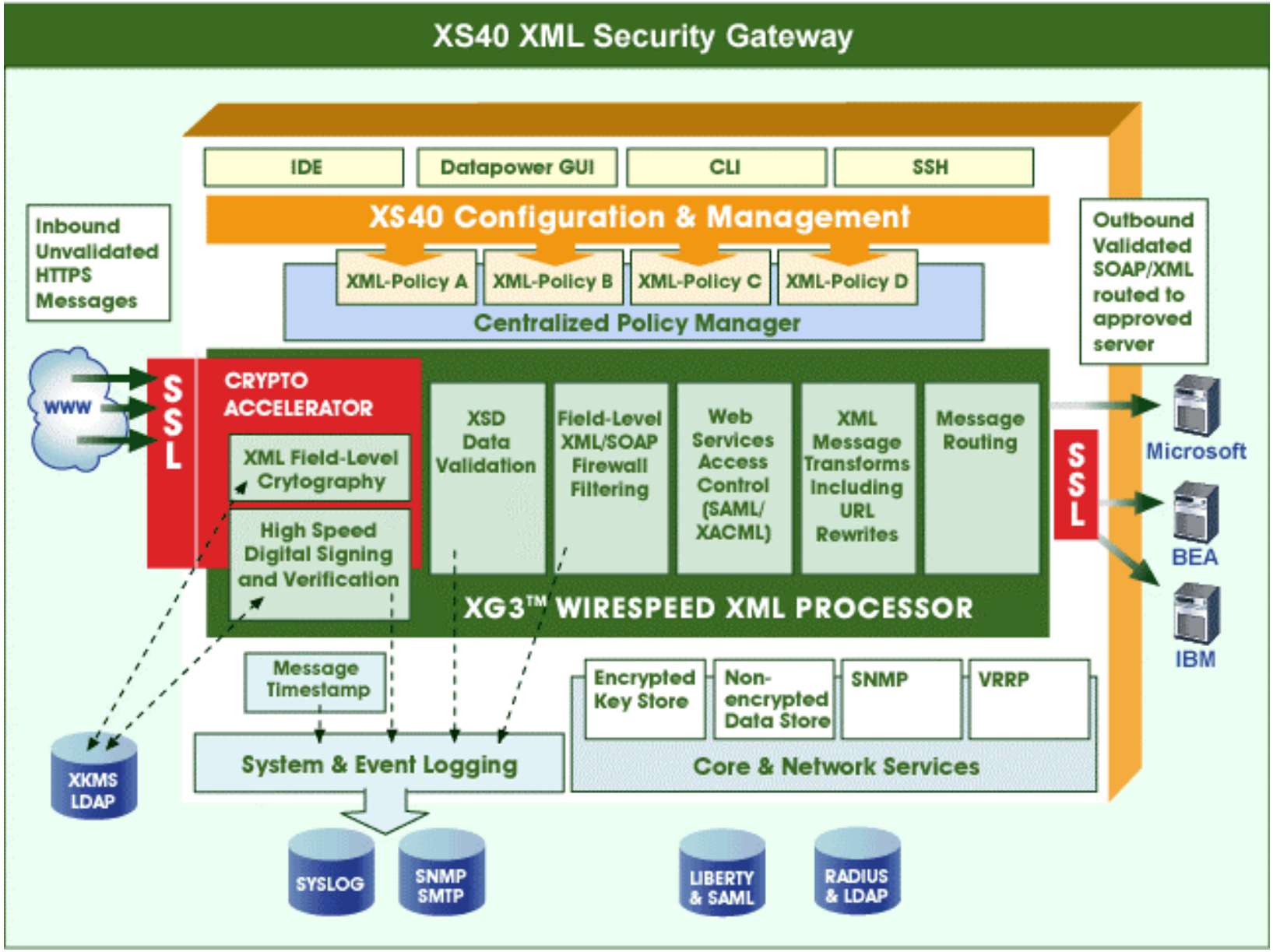
Stephen Roche
CTO of Hemscott



Hemscott provides TD Waterhouse with hosted web pages which are seamlessly integrated into the TD Waterhouse website as part of its online trading service.

XML Security Gateway Deployment & Features




XS40 XML Security Gateway
IDE
Datapower GUI
CLI
SSH
XS40 Configuration & Management
XML-Policy A
XML-Policy B
XML-Policy C
XML-Policy D
Centralized Policy Manager
Inbound Unvalidated HTTPS Messages
Outbound Validated SOAP/XML routed to approved server
WWW
SSL
CRYPTO ACCELERATOR
XML Field-Level Crytography
High Speed Digital Signing and Verification
XSD Data Validation
Field-Level XML/SOAP Firewall Filtering
Web Services Access Control (SAML/ XACML)
XML Message Transforms Including URL Rewrites
Message Routing
XG3™ WIRESPEED XML PROCESSOR
SSL
Microsoft
BEA
IBM
Message Timestamp
Encrypted Key Store
Non-encrypted Data Store
SNMP
VRRP
System & Event Logging
Core & Network Services
XKMS LDAP
SYSLOG
SNMP SMTP
LIBERTY & SAML
RADIUS & LDAP

DataPower

XML-Aware Network Services

- New “in-the-network” services for WS
- Directories/registries of web services, UDDI, etc.
- Edge processing and acceleration
- Guaranteed delivery of XML docs & transactions
- Cryptographic tokens and PKI certificates
- Managed security service providers for WS
- Fully outsourced deployment infrastructure

Conclusion

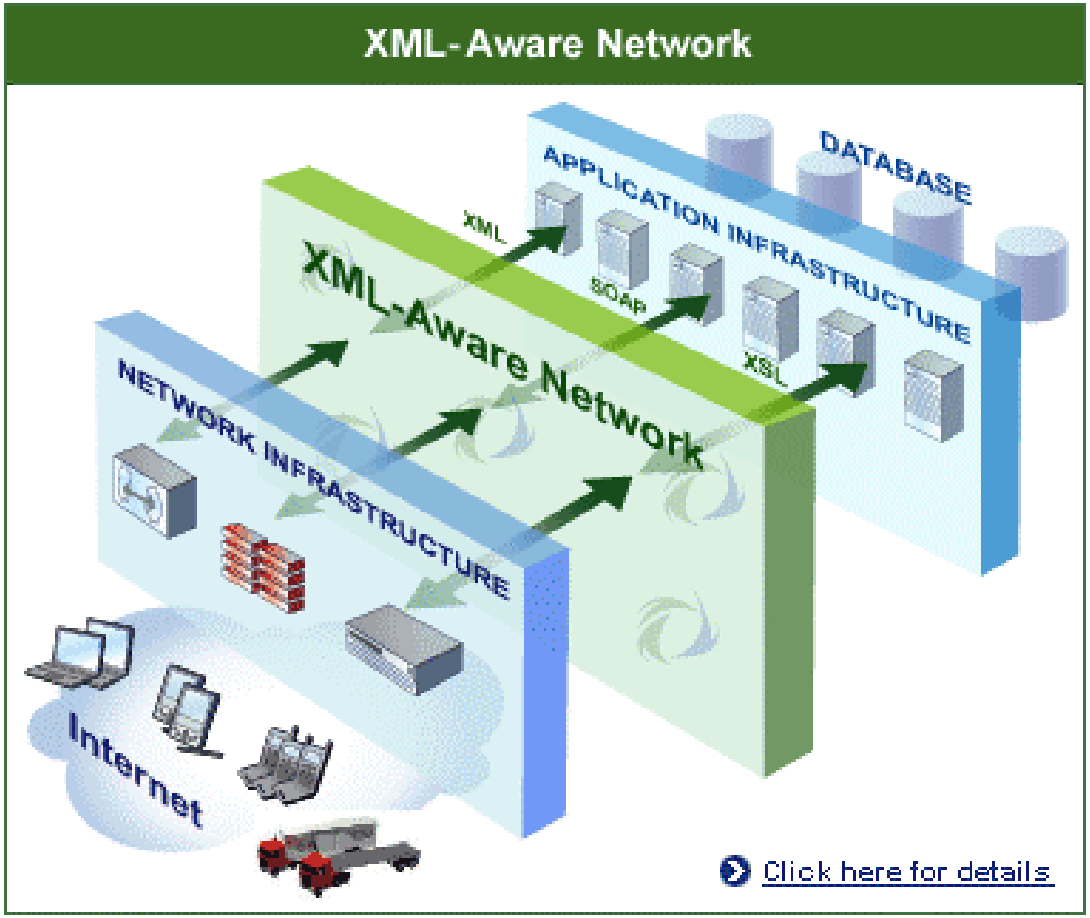
- **Bad**
  - Bottlenecks introduced by nature of XML
  - Securing heterogeneous apps difficult
  - XML security & performance can cost a lot of money → wiping out savings from using
- **Good**
  - XML can reduce costs
  - A novel (XAN) approach exists!
  - Good products exist
- **Conclusions**
  - Separate security & acceleration from the application logic
  - Centralize security in network
  - Use XAN to make XML Web Services FASTER, SAFER and CHEAPER

Q & A

Eugene Kuznetsov
Chairman & CTO
DataPower Technology, Inc.
http://www.datapower.com

DATAPOWER

XML-aware Network Infrastructure



The

- Performance
- Security
- Manageability

that you expect from your IP network for your XML apps

DataPower

Some Technical Notes

- Using existing string matching / deep packet filtering
  - Example, look for “<foo>” in first 200 bytes
  - Problem #1: often hard limit on # of bytes
  - Problem #2: unaware of XML tree structure
  - Problem #3: no single canonical form (<foo/> or Unicode)
- Caching for performance
  - Caching technology to avoid XSLT delays
  - Caching for web services … ?
- Performance challenges
  - Much more complex processing than previously attempted
  - Wirespeed is the network standard

More Technical Notes

- Security via same engine/system as endpoint
  - Example, XML filtering
  - Problem #1: same vulnerability will affect FW as host
  - Problem #2: different requirements for technology
- Tightly coupled systems
  - Example, platform code in XML processing
  - Problem #1: not web services way!
  - Problem #2: makes migration of function into network difficult

XS40 Secures RouteOne Auto Credit Applications

- Innovative app links 22,000 dealers to financing sources
- Loan applications secured with no performance degradation

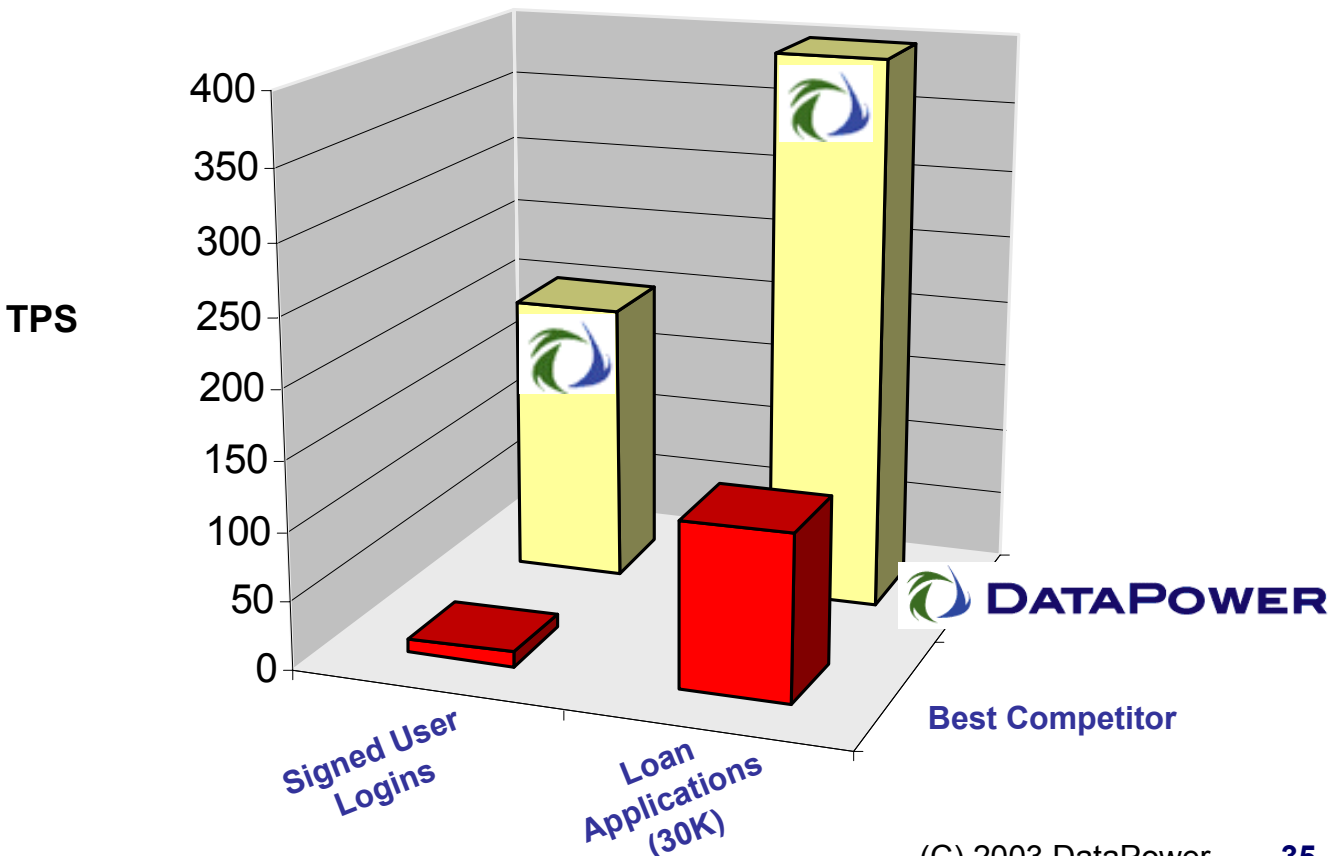
RouteOne

DaimlerChrysler

GMAC Financial Services

Toyota Financial Services

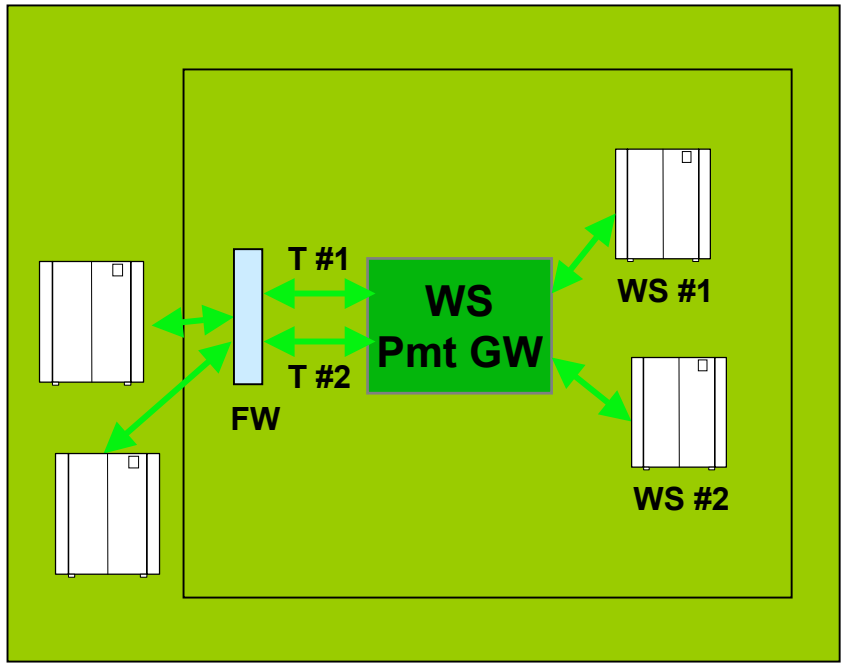
Ford Credit



DataPower

WS Payment/Billing GW

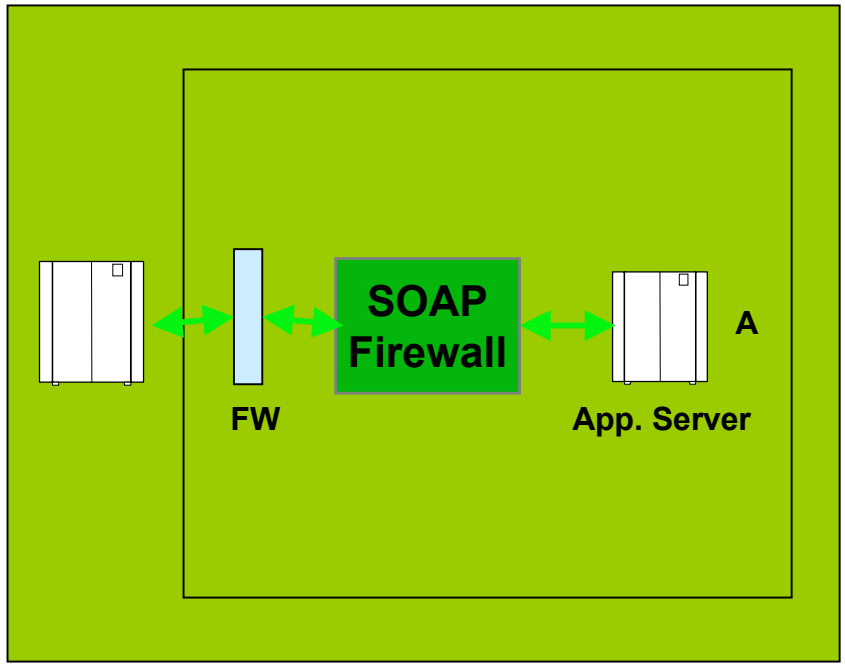
- Token-based web services payments
- Tokens as authorizations for specific web service use: T#1-> WS1, T#2->WS2
- Based on XML-DSIG, PKI, XKMS & crypto → difficult to deploy across all servers
- GW provides a centralized access point to all web service end nodes
- Dedicated, central point of access control and management: PnP revenue



DataPower

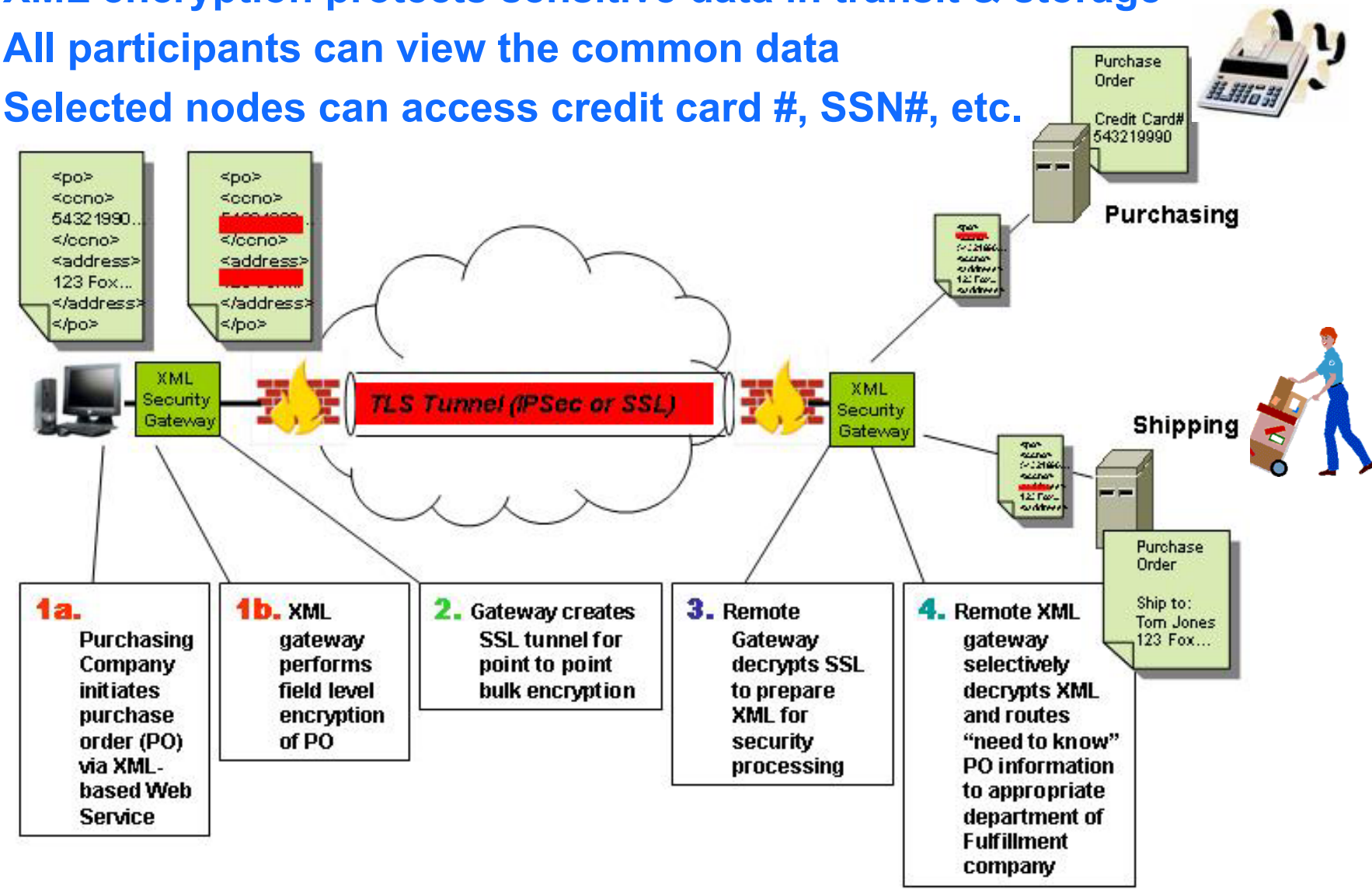
XML (or SOAP) Firewall

- Intercepts incoming & outgoing WS requests
- Augments or incorporates IP-layer firewall
- Checks for well-formed XML
- Performs XML DoS checks
- Validates against standard (e.g. SOAP) or custom user schemas
- Applies XPath or similar rules
- Integrates with access control solution



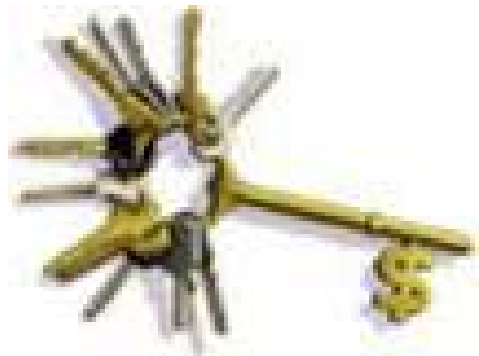
What to Encrypt?

- XML encryption protects sensitive data in transit & storage
- All participants can view the common data
- Selected nodes can access credit card #, SSN#, etc.



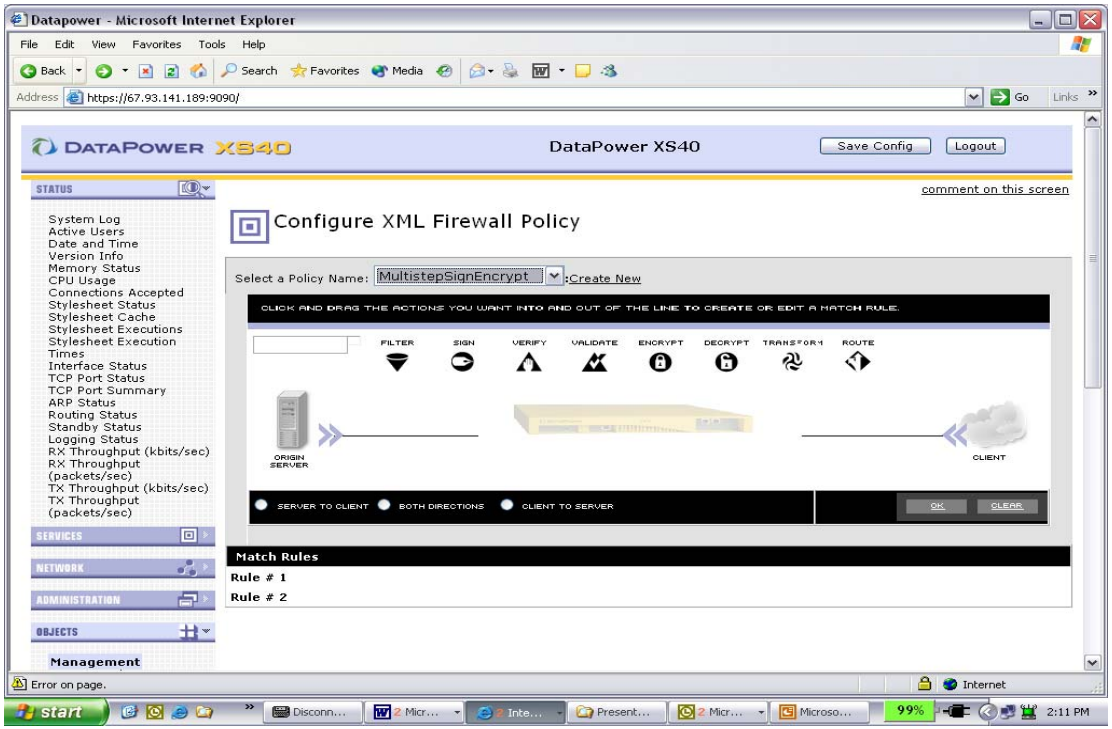
PKI is Hard

- PKI-enabling apps is difficult
  - CRL, OCSP, X.509, ASN.1…
- Securing keys is difficult
  - Software keys on general machines easy to find, easy to steal
  - Integration with crypto devices not always practical
- Why deploy just crypto device?
- Deploy an XML Security Device
  - Applied crypto for all XML applications



XS40 XML Security Gateway

Ease of Use



- **Drag & drop firewall actions!**
- **Configure and install in minutes**
- **Full IDE support for advanced XML-based configuration**

Ease of Use Example – Graphical User Interface providing drag and drop services, in order desired, for XML filtering, signing, verification, validation, encryption, decryption, transformation and routing